ILME-FX6

ข้อควรระวังด้านความปลอดภัย

คู่มือช่วยเหลือนี้อธิบายข้อควรระวังด้านความปลอดภัยสำหรับการโอนย้ายไฟล์และการสตรีมมิ่งโดยใช้เครื่อง

ILME-FX6
ข้อควรระวังด้านความปลอดภัย

ข้อควรระวังด้านความปลอดภัย

หัวข้อนี้อธิบายข้อควรระวังเมื่อเชื่อมต่อเครื่องกับเครือข่าย

- อาจมีการลอบดักฟังข้อมูลการสื่อสารโดยบุคคลที่สามที่ไม่ได้รับอนุญาตภายในบริเวณของสัญญาณ เมื่อใช้การสื่อสารผ่าน LAN แบบไร้สาย โปรดใช้มาตรการด้านความปลอดภัยที่เหมาะสมเพื่อปกป้องข้อมูลที่มีการสื่อสาร
- หากคุณตั้งค่า [Security] ในการตั้งค่า LAN แบบไร้สายเป็น [None] และเชื่อมต่อกับจุดเชื่อมต่ออินเทอร์เน็ต การสื่อสารไร้สายระหว่างกล้องและจุดเชื่อมต่ออินเทอร์เน็ตจะไม่ได้รับการเข้ารหัสและอาจถูกดักจับโดยบุคคลที่สามภายในระยะสัญญาณ ใช้โปรโตคอลความปลอดภัย WPA2 หรือ WPA3 เพื่อเพิ่มความปลอดภัย
- SONY จะไม่รับผิดต่อความเสียหายไม่ว่าจะในรูปแบบใดที่เป็นผลมาจากการไม่สามารถนำมาตรการด้านความปลอดภัยที่เหมาะสมมาใช้กับอุปกรณ์รับส่งสัญญาณ การรั่วไหลของข้อมูลที่ไม่สามารถหลีกเลี่ยงได้เนื่องจากข้อมูลจำเพาะในการรับส่งข้อมูล หรือปัญหาด้านความปลอดภัยไม่ว่าจะเป็นในรูปแบบใดก็ตาม
- บุคคลที่สามที่ไม่ได้รับอนุญาตบนเครือข่ายอาจสามารถเข้าใช้เครื่องได้ แต่ทั้งนี้ให้ดูจากสภาพแวดล้อมในการทำงานเป็นสำคัญ เมื่อเชื่อมต่อเครื่องเข้ากับเครือข่าย ต้องแน่ใจว่าเครือข่ายได้รับการป้องกันอย่างรัดกุมแล้ว
- เมื่อเชื่อมต่อผลิตภัณฑ์เข้ากับเครือข่าย โปรดเชื่อมต่อผ่านระบบที่มีฟังก์ชันรักษาความปลอดภัย เช่น เราเตอร์หรือไฟร์วอลล์ หากเชื่อมต่อโดยไม่มีระบบป้องกันเหล่านี้ อาจเกิดปัญหาเรื่องความปลอดภัยขึ้นได้

TP1002274654

ILME-FX6
ข้อควรระวังด้านความปลอดภัย

ข้อควรระวังในการเชื่อมต่ออินเทอร์เน็ต

หัวข้อนี้อธิบายข้อควรระวังเมื่อเชื่อมต่อเครื่องกับอินเทอร์เน็ต

- เครื่องไม่สามารถเชื่อมต่อผ่าน LAN แบบไร้สายกับจุดเชื่อมต่ออินเทอร์เน็ตที่ใช้เฉพาะ WEP หรือ WPA เท่านั้น ซึ่งเป็นวิธีการรักษาความปลอดภัยที่มีช่องโหว่
- เครื่องนี้ไม่ใช่อุปกรณ์เครือข่าย (เช่น เราเตอร์หรือสวิตชิ่งฮับ) ขอแนะนำอย่างยิ่งให้คุณเชื่อมต่อเครื่องเข้ากับเครือข่ายที่คุณสามารถกำหนดค่าและจัดการการตั้งค่าเครือข่ายได้อย่างเหมาะสม เพื่อป้องกันการโจมตีบนเครือข่าย เช่น การโจมตี DoS (การโจมตีปฏิเสธบริการ)
- เมื่อเชื่อมต่อเครื่องกับเครือข่าย ให้เชื่อมต่อผ่านเราเตอร์ที่ได้รับการกำหนดค่าและจัดการอย่างเหมาะสม หรือเชื่อมต่อกับพอร์ต LAN ที่มีฟังก์ชันการทำงานเดียวกัน หากเชื่อมต่อโดยไม่มีการป้องกันดังกล่าว (เช่น เมื่อใช้ Wi-Fi ฟรี) อาจเกิดปัญหาด้านความปลอดภัยได้ เมื่อกำหนดค่าอย่างถูกต้องแล้ว เราเตอร์จะให้การป้องกันที่เพียงพอต่อการโจมตี DoS หรือการสูญเสียการทำงานของอุปกรณ์ในเครือข่าย หากคุณสังเกตเห็นสิ่งผิดปกติ ให้ตัดการเชื่อมต่อกล้องจากเครือข่ายทันที

TP1002274655

ILME-FX6
ข้อควรระวังด้านความปลอดภัย

ข้อควรระวังเกี่ยวกับฟังก์ชันเครือข่าย

หัวข้อนี้อธิบายข้อควรระวังเกี่ยวกับฟังก์ชันเครือข่ายของเครื่อง

- หากตรวจพบการเข้าถึงที่ไม่ได้รับอนุญาต กล้องอาจไม่สามารถรับการสื่อสารได้ หากเกิดเหตุการณ์นี้ขึ้น ให้เชื่อมต่อใหม่ตั้งแต่ต้น
- กดปุ่ม [Show Authentication] บนหน้าจอสถานะ [Network] เพื่อแสดงข้อมูลการยืนยันตัวตนสำหรับการเชื่อมต่อกับตัวเครื่อง ระมัดระวังอย่าให้ผู้อื่นเห็นหน้าจอและคัดลอกภาพรหัส QR ได้
- ชื่อผู้ใช้และรหัสผ่านจะถูกสร้างขึ้นและตั้งค่าบนกล้องโดยอัตโนมัติ ณ เวลาที่ซื้อ เมื่อตั้งชื่อผู้ใช้และรหัสผ่านของคุณ ตรวจสอบให้แน่ใจว่าการตั้งค่าดังกล่าวจะไม่ปรากฏให้ผู้อื่นเห็น ตั้งชื่อผู้ใช้และรหัสผ่านดังต่อไปนี้

[User Name]	– ตั้งชื่อผู้ใช้โดยมีความยาว 1 ถึง 16 อักขระ – ค่าเริ่มต้นที่ตั้งไว้คือ “admin” – อักขระอินพุตที่ถูกต้องมีดังต่อไปนี้ อักขระตัวอักษร (ตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก) อักขระตัวเลข สัญลักษณ์ (! % + , - . = _)
[Password]	– ตั้งรหัสผ่านโดยมีความยาว 8 ถึง 16 อักขระ ต้องมีตัวอักษรอย่างน้อย 1 ตัวขึ้นไปและตัวเลขอย่างน้อย 1 ตัวขึ้นไป – อักขระอินพุตที่ถูกต้องมีดังต่อไปนี้ อักขระตัวอักษร (ตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก) อักขระตัวเลข สัญลักษณ์ (! % + , - . = _)

TP1002274656

ILME-FX6
ข้อควรระวังด้านความปลอดภัย

ข้อควรระวังที่เกี่ยวข้องกับ LAN แบบไร้สาย

หัวข้อนี้อธิบายข้อควรระวังเมื่อเชื่อมต่อเครื่องผ่าน LAN แบบไร้สาย

- ในคู่มือช่วยเหลือสำหรับเครื่องนี้ จุดเชื่อมต่ออินเทอร์เน็ตด้วย LAN แบบไร้สายและเราเตอร์ LAN แบบไร้สายที่ถ่ายทอดการเชื่อมต่อ LAN เรียกว่า “จุดเชื่อมต่ออินเทอร์เน็ต”
- [Security] (วิธีการเข้ารหัส) สามารถตั้งเป็น [None], [WPA2] หรือ [WPA3] แนะนำให้ใช้ [WPA2] หรือ [WPA3] จากมุมมองในเรื่องความปลอดภัย เมื่อเลือก [None] ข้อความจะแสดงขึ้นก่อนการเชื่อมต่อ สำหรับการเชื่อมต่อ LAN แบบไร้สายที่ปลอดภัย ขอแนะนำเป็นอย่างยิ่งให้เชื่อมต่อกับจุดเชื่อมต่ออินเทอร์เน็ตด้วยการตั้งค่าความปลอดภัย WPA2 หรือ WPA3
- โดยค่าเริ่มต้นจะเลือกวิธีการรักษาความปลอดภัย WPA2 เมื่อลงทะเบียนจุดเชื่อมต่ออินเทอร์เน็ตด้วย LAN แบบไร้สายโดยใช้ [Manual Register]
- หากคุณเชื่อมต่อกับจุดเชื่อมต่ออินเทอร์เน็ตโดยไม่มีการตั้งค่าความปลอดภัยใดๆ คุณอาจถูกแฮ็ก เข้าถึงโดยบุคคลภายนอกที่ไม่หวังดี หรือถูกโจมตีจากช่องโหว่ต่างๆ ไม่แนะนำให้เชื่อมต่อโดยไม่มีการตั้งค่าความปลอดภัยใดๆ เว้นแต่จะหลีกเลี่ยงไม่ได้
- การกำหนดค่าความปลอดภัยบน LAN แบบไร้สายเป็นสิ่งสำคัญมาก Sony จะไม่รับผิดชอบต่อความเสียหายใดๆ ที่เกิดจากการไม่ดำเนินมาตรการรักษาความปลอดภัย หรือหากเกิดปัญหาความปลอดภัยเนื่องจากสถานการณ์ที่ไม่อาจหลีกเลี่ยงได้ในการใช้งาน LAN แบบไร้สาย

TP1002274657

ILME-FX6
ข้อควรระวังด้านความปลอดภัย

ข้อควรระวังที่เกี่ยวข้องกับการเชื่อมต่อด้วย USB

หัวข้อนี้อธิบายข้อควรระวังเมื่อเชื่อมต่อเครื่องผ่านการเชื่อมต่อด้วย USB

- ใช้เฉพาะอุปกรณ์สมาร์ทโฟนที่เชื่อถือได้สำหรับการเชื่อมต่อ ไม่แนะนำให้เชื่อมต่อกับอุปกรณ์ที่มีแหล่งที่มาที่ไม่รู้จักเนื่องจากข้อกังวลด้านความปลอดภัย

TP1002274658

ILME-FX6
ข้อควรระวังด้านความปลอดภัย

เกี่ยวกับฟังก์ชัน FTPES (FTPS)

ฟังก์ชัน FTPS รองรับอัลกอริทึมการเข้ารหัสต่างๆ เพื่อให้มั่นใจถึงการโอนย้ายไฟล์ที่ปลอดภัย รองรับอัลกอริทึมการเข้ารหัสหลายแบบ ซึ่งบางแบบอาจไม่สอดคล้องกับแนวทางปฏิบัติด้านความปลอดภัยที่ดีที่สุดในปัจจุบัน เพื่อให้เข้ากันได้กับเซิร์ฟเวอร์ที่หลากหลาย

อัลกอริทึมการเข้ารหัสที่รองรับโดยฟังก์ชัน FTPS

อัลกอริทึมการเข้ารหัสที่รองรับมีดังต่อไปนี้

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

อัลกอริทึมการเข้ารหัสที่แนะนำ

แนะนำให้ใช้อัลกอริทึมการเข้ารหัสต่อไปนี้ตามคำแนะนำของ NIST (NIST SP 800-57 Part 1 Revision 5) และมาตรฐานความปลอดภัยที่เกี่ยวข้อง

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

เกี่ยวกับอัลกอริทึมที่เลิกใช้แล้ว

ฟังก์ชัน FTPS ยังรองรับอัลกอริทึมความเข้ากันได้ต่อไปนี้ แต่จะไม่รองรับอีกต่อไปตามคำแนะนำของ NIST (NIST SP 800-57 Part 1 Revision 5) และมาตรฐานความปลอดภัยที่เกี่ยวข้อง และอาจถูกลบออกในเวอร์ชันถัดไป

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

เกี่ยวกับความเข้ากันได้ของการเชื่อมต่อ

ฟังก์ชัน FTPS ได้รับการออกแบบให้มีความสมดุลระหว่างความปลอดภัยและความเข้ากันได้ ปัจจุบัน อัลกอริธึมที่เลิกใช้แล้วได้รับการรองรับด้วยเหตุผลต่อไปนี้ แต่อาจถูกลบออกในเวอร์ชันถัดไปเพื่อปรับปรุงความปลอดภัย

- ช่างภาพและช่างวิดีโออิสระจำเป็นต้องเชื่อมต่อกับเซิร์ฟเวอร์ที่ทำงานบนไคลเอนท์ต่างๆ

- จำเป็นต้องรักษาความเข้ากันได้กับระบบเก่าและเซิร์ฟเวอร์เดิม
- ผู้ใช้บางรายอาจไม่พร้อมที่จะเปลี่ยนเป็นการตั้งค่าที่ปลอดภัยยิ่งขึ้น เนื่องจากการเปลี่ยนการตั้งค่าอัลกอริทึมการเข้ารหัสทางฝั่งเซิร์ฟเวอร์มีความซับซ้อน
- การตั้งค่า FTPS มักถูกแชร์กับบริการที่ปลอดภัยอื่นๆ การเปลี่ยนแปลงใดๆ จะต้องได้รับการพิจารณาอย่างรอบคอบเนื่องจากอาจส่งผลกระทบต่อบริการอื่นๆ บนเซิร์ฟเวอร์
- จะต้องรองรับอัลกอริทึมการเข้ารหัสที่หลากหลายเพื่อให้แน่ใจว่าสามารถทำงานร่วมกันได้ในสภาพแวดล้อมที่แตกต่างกัน

อัลกอริทึมการเข้ารหัสที่ใช้ในระหว่างการเชื่อมต่อ FTPS ถูกกำหนดโดยการเจรจาอัตโนมัติกับเซิร์ฟเวอร์ปลายทาง ดังนั้นจึงขึ้นอยู่กับการตั้งค่าเซิร์ฟเวอร์ แม้จะตระหนักถึงความเสี่ยงด้านความปลอดภัย แต่ความเข้ากันได้เป็นสิ่งสำคัญที่สุดเพื่อตอบสนองความต้องการที่หลากหลายของผู้ใช้

ความเสี่ยงด้านความปลอดภัย

การใช้อัลกอริธึมที่เลิกใช้แล้ว รวมถึง CBC/DHE/RSA/SHA-1 จะเพิ่มความเสี่ยงที่ข้อมูลที่เข้ารหัสอาจถูกถอดรหัสหรือดัดแปลงโดยผู้โจมตี และส่งผลให้ข้อมูลถูกเปิดเผยระหว่างการโอนย้าย

คำแนะนำสำหรับการเชื่อมต่อที่ปลอดภัย

ก่อนใช้ฟังก์ชัน FTPS ให้ตรวจสอบว่าเซิร์ฟเวอร์ปลายทางการเชื่อมต่อรองรับอัลกอริทึมการเข้ารหัสที่แนะนำหรือไม่ เปิดใช้งานเฉพาะอัลกอริทึมที่แนะนำบนฝั่งเซิร์ฟเวอร์ และปิดใช้งานอัลกอริทึมที่เลิกใช้แล้ว

การอัพโหลดโดยใช้ FTP ที่ปลอดภัย

คุณสามารถอัพโหลดไฟล์ที่มีการเข้ารหัสลับไว้โดยใช้ FTPS ในโหมด Explicit (FTPES) เพื่อเชื่อมต่อกับเซิร์ฟเวอร์ไฟล์ปลายทางสำหรับการโอนย้ายด้วย FTP ที่ปลอดภัย ให้ตั้ง [Using Secure Protocol] เป็น [On] ในการตั้งค่าเซิร์ฟเวอร์ปลายทางการโอนย้ายไฟล์ และนำเข้าใบรับรอง

การอ้างอิง

- Recommendation for Key Management, Special Publication 800-57 Part 1 Revision 5, NIST, 2020.
- Transitioning the Use of Cryptographic Algorithms and Key Lengths, Special Publication 800-131A Revision 2, NIST, 2019.
- Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, NIST, 2005 (รวมถึงการปรับปรุง ณ วันที่ 10/06/2016).

ใบรับรอง

เขียนใบรับรองโดยใช้ฟังก์ชัน FTPES (FTPS) ไปยังไดเรกทอรีรากของการ์ดความจำ ตั้งชื่อไฟล์ดังต่อไปนี้
certification.pem (รูปแบบ PEM)
ขนาดใบรับรองสูงสุดที่สามารถโหลดได้คือ 1 MB ต่อใบรับรอง

TP1002274659